REMARKS

Claim Amendments

Claims 1, 2, 4, 6-10, 12, 13 and 15-18 are now pending in this application.

Independent system claim 1 (and in like manner, independent method claim 10) has been amended and defines an electronic document management system for verifying the contents of an electronic document exchanged through a network, wherein the contents defines the electronic document and comprises a predetermined electronic form template and variable data input by a user, including:

(a) at least one data storage means for storing said user-input variable data and said template;

(b) a data capturing component for capturing and validating said user-input variable data, and forwarding said validated variable data to said storage means;

(c) a document digest generator for generating a unique document digest from said stored user-input variable data and said template defining said electronic document by applying a secure algorithm thereto, whereby said document digest is uniquely associated with said defined electronic document, and forwarding said document digest to said storage means for storage in association with said defined electronic document;

(d) a barcode generator for generating for each page of said electronic document a unique barcode associated with that specific page, based on paging details identifying said page and said document digest;

(e) a document forwarding component for forwarding said defined electronic document with each said unique barcode added to said specific page of said electronic document associated therewith for use by a user;

(f) a document receiving component for receiving from a user a signed electronic document comprising variable data and a barcode for each page of said document; and,

(g) a barcode verification component for determining the validity of each said barcode of said received electronic document wherein a said document digest component of said barcode is compared to said stored document digest associated with said defined electronic document.

35 U.S.C. §103(a) Rejections

Applicant respectfully requests reconsideration and withdrawal of the claim rejections by the Examiner having regard to the following submissions.

The Examiner has indicated that claims 1-5 and 10-14 are rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over U.S. patent No. 5,606,609 ("Houser et al.") in view of U.S. published patent application No. 2002/0188845 ("Henderson et al."). Further, the Examiner has indicated that claims 6-9 and 15-18 are rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Houser et al. and Henderson et al., and further in view of Adobe Acrobat 3.0 Tutorial ("Adobe").

As dictated in MPEP 2143, in order to establish a prima facie case of obviousness, the Examiner must be satisfied that three requirements have been established: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of

success; and thirdly, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

With respect to the first requirement, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art. The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art. Additionally, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. Although a prior art device may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so.

For the following reasons Applicant respectfully submits that Houser et al. and Henderson et al. and/or Adobe do not disclose, teach or even suggest applicant's invention whether viewed alone or in combination. Further, there is no motivation to modify these references to provide the features of independent claim 1 of this application.

The cited patent to Houser et al. provides a system and method for verifying and indicating the integrity, source and/or approval status of an electronic document, wherein security information is captured in a security object and that security object, which also contains an identifier to invoke processing of the security information, is embedded in the document at a user's request to effect that user's signing or approval of the document. The objective is to provide means for computer application users to "sign" (i.e. signal their approval) a document in a relatively secure manner before sending it to others over the Internet in such manner that recipients of the documents may confirm that user's approval and the exact document so approved.

More specifically, Houser et al. provide an installer which adds menu items to windows applications such as Word or Excel whereby a user makes a request to 'sign' an electronic document through these menu items and, when the request is made, a security object is embedded in the electronic document (an OLE 2.0 object). The security object may be encrypted according to public or private key encryption and may contain a document digest, which includes data items that characterize the electronic document at the time the security object is embedded, or a signature digest which includes data items that characterize the signator. Also, the security object may contain a serial number which is unique for each embedded security object and may contain an electronic chop associated with the user who embedded the security object which is displayed only if the signed electronic document is verified (e.g. a watermark graphic can be generated in the electronic document if the signed electronic document is verified).

The cited published patent application of Henderson et al. provides a system and method for generating and validating value-bearing documents. The intention of Henderson et al. is to improve the security of encrypted documents by using a set of encryption keys, as opposed to a single encryption key, so that, if one key is compromised, the security of only a subset of documents will be put at risk. A barcode is used by the system of Henderson et al. only to be able to automatically recognize the document in question and not, as in applicant's invention, as a means to identify whether the document is authentic together with a person's signature applied thereto.

In Henderson et al.'s system a user requests a value-bearing document (ticket, coupon, gift certificate) and, in response, an issuer module creates a value-bearing document containing start and stop dates and forwards the document to a guarantor module. The guarantor module generates a message containing the encrypted document by selecting an encryption key from a pre-determined set of keys and using that key to encrypt the value-bearing document. To guarantee the integrity of the document, the guarantor also computes a hash or message digest of the encrypted document which is then itself encrypted and the encrypted message digest is concatenated to the encrypted value-

bearing document (referred to a the payload). The guarantor creates an options field and attaches it to the payload and an encryption scheme index to the message. It then adds a length field to the message, which may be converted to ASCII format or into bar code format. The message is returned to the user (requestor) via the issuer module and a validator extracts the length, the encryption scheme index and the options value. The validator extracts the encrypted document from the received message and retrieves the encryption key corresponding to the index, calculates the digest of the extracted encrypted document, extracts the message digest, decrypts it and compares it to the calculated message digest. If the digests match, the validator proceeds to decrypt the document using the key and it may validate the document's contents using the start and stop dates.

By contrast with applicant's claimed invention, neither Houser et al. nor Henderson et al. contemplate any means (or, indeed, any need) for authenticating the creation of the document. Rather, they deal with the finished document per se after it has been fully rendered. Nor are they capable of authenticating a hand-signed document (as distinguished from the wholly electronically processed documents of Houser et al. and Henderson et al), for which there is an added security risk and complication presented by the fact that individual pages may be substituted to alter an original document (i.e. with the alteration being cleverly done to produce the same single, overall document digest based on a post-rendering of the document). Also in contrast with applicant's invention, neither of Houser et al. and Henderson et al. discloses or contemplates means to identify and track the changes made to an electronic document during its lifecycle.

Applicant's system authenticates the creation of the document and provides separate unique barcodes for authenticating the document on a page-by-page basis at the time the document is rendered (created). It authenticates the creation of the document, at the outset, by validating the user-input variable data (see page 4, line 24; page 5, line 3; page 8, lines 26-27) which is input by a user into a predetermined electronic form template. Therefore, any limitations or constraints applicable to that variable data, that are not complied with by the user-input variable data, can be rejected at the outset to prevent

introduction to the system of a non-conforming document. For example, with reference to Figure 2 of applicant's subject application, and the user-variable input data for "Effective Date", the user-input data validation performed by the system may require, in the context of that particular template, that this date must be after "x" but before "y".

Following this validation of the user-input variable data, the applicant's system then takes that variable data and the predetermined document form template into which that variable data was entered and processes these content items specific to that document (which define the document) by applying to them a hash algorithm to produce a unique document digest (digital hash). Then, as part of the process of creating the document (i.e. to render the document complete), that unique document digest and paging details identifying a specific page of the document (see page 7, lines17-23; page 9, lines 2-4) are combined to produce a unique barcode (document identifier) for each such specific page of the document. Thus, each page is associated with its own unique identifier - being unique to that particular page of the document - upon the creation of the document. Preferably, historical data about that document (viz. its revision number) and the unique document number for the document are also combined with the paging details for each specific page to form the barcode for that page.

Houser et al. does not address the creation of the document or the security risk posed by separation of the document pages. Moreover, Houser et el. cannot provide the unique barcode identifiers of applicant's invention because they cannot be produced after the document is rendered and, to the contrary, must be produced during the creation of the document per the foregoing. The Examiner states in the Office Action that "it would have been obvious hand sign and fax a document in order to verify that somebody has approved the document" but, in fact, the system of Houser et al. not only does not allow for (or contemplate) this, but it provides no motivation to do so. To the contrary, Houser et al. teaches away from such because it does not provide any security measures which could allow for this to happen; it deals with the already rendered electronic document, as a whole, without any distinction being made to the pages of the document or the security of

those individual pages. Houser et al. only authenticates "acts" signifying a user's signing of a document, electronically, using digital signatures which are authenticated by a third party digital certification engine (a public/private key system). Whereas, applicant's invention retains the existing process of paper documents being signed and/or initialed and, in many cases, dated by the author using a pen or other indelible marker, whereby the signature manifests his or her approval of the document as it exists at that time. This can be important because where needed, at a later time, the authenticity of that physical signature can be evaluated (confirmed) by an expert, the signatory, or another person familiar with the signature, so as to verify the physical signature on the signed document.

Nor does Henderson et al. Moreover, applicant's system can recreate the document at any point of its lifecycle (history), via its unique document number and revision number, which Houser et al. cannot do (and does not contemplate).

By reason of the foregoing amendments to the independent claims, applicant respectfully submits that the pending claims patentably distinguish over the prior art and are in good form for allowance. Applicant notes that if independent claims 1 and 10 are non-obvious under 35 USC 103 then any claim depending therefrom is non-obvious [see In re Fine, 5 USPQ2d 1596 (Fed. Cir. 1988)].

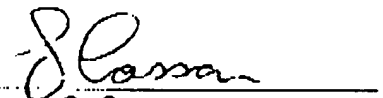
CONCLUSIONS

For all the foregoing reasons, Applicant respectfully submits that all pending claims, as amended herein, are in good order and ready for allowance. Reconsideration and withdrawal of the objections raised in the first Office Action is respectfully requested. In the event that the Examiner cannot allow the present application for any reason, the Examiner is encouraged to contact applicant's attorney to discuss resolution of any

remaining issues.

Dated this 4th day of March, 2005.

Respectfully submitted,
SHAWN L. KING



Lynn S. Cassan
Attorney for Applicant
Registration No. 32,378

CASSAN MACLEAN
Suite 401 - 80 Aberdeen St.
Ottawa, Ontario
Canada K1S 5R5
Telephone: (613) 238-6404